Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

WHITE PAPER SERIES

Extremist Use of Social Media and Encrypted Messaging Applications

September 2019

INTENT

This white paper is designed to provide analysis of relevant, publicly available information on threat and hazard events/trends and their potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be an all-encompassing assessment of the subject.

Extremist Use of Social Media and Encrypted Messaging Applications

Introduction

Extremist groups now have constant access to a global audience through relatively simple and free technology. Furthermore, depending on the platform, some messages may not be monitored, filtered, or potentially traced back to the initial source. Groups such as the Islamic State (IS) have used social media accounts to recruit new members and spread propaganda. Encrypted messaging apps are then used to maintain an information network, at times conveying plans and information related to attacks. Traditionally domestic groups, in particular far-right extremists, have also begun to spreading information and propaganda via communication platforms such as Twitter and Telegram, reaching outside of the country of origin to a global audience.

Social Media

A number of popular social media platforms such as Facebook, YouTube, Tumblr, and Twitter have been utilized in the past by terrorist groups to spread propaganda and promote fear. These sites are cheap and accessible to a massive audience. While such accounts typically violate the platforms' terms of service, companies have struggled to monitor and remove this content.[11,12]

Twitter

Until 2016, Twitter was the online platform of choice for English-language Islamic State (IS) sympathizers. As a result of Twitter's counter-extremism policies (including content removal) there has been a decline in activity by IS supporters. While Twitter does attempt to monitor and shut down accounts that "threaten or promote terrorism or violent extremism," it is still utilized by a variety of extremists to spread propaganda, promote recruitment, and claim credit for attacks. Groups such as Al-Shabab, Hezbollah, Hamas, the Taliban, and IS post frequently on Twitter, though the accounts may be at times suspended.[11]

8chan

8chan is an open message board with minimal restrictions on content sharing. Portions of the site have become havens for far-right extremists. Propaganda from white nationalists could frequently be found. In 2019, three mass shootings were preceded by the posting of a manifesto on 8chan: The New Zealand Mosque shooting, the San Diego synagogue shooting, and the El Paso shooting. Posting these manifestos to 8chan before a mass shooting enabled the attackers to gain attention and amplify their message. Following these shootings, 8chan was removed from Clearnet in August. However, far-right extremists have begun moving to alternate platforms such as Gab. Additionally, users continue to access the site through its IP address and via its .onion address on the darknet.[8,9]

Encrypted Messaging

Some communication platforms like Telegram, WhatsApp, and Signal use end-to-end encryption. This type of encryption converts messages into a code without the help of a server in the middle,

making it nearly impossible to gain access to communication between two users without their consent. The message is scrambled so that it becomes indecipherable to anyone but its intended recipient when it is sent, and it remains so when it passes through the app's server and reaches the recipient. Extremist groups exploit these applications and their privacy and security policies to securely share information between members.

Telegram

Telegram is a multimedia messaging application that is accessible by smartphones, tablets, and computers. Telegram users can share an unlimited number of photos, videos, documents, audio messages, and voice recordings in four different communication options: direct one-to-one secret chats and voice calls, groups and supergroups that can include as many as 200,000 members, and channels that broadcast to a theoretically unlimited number of users. Telegram users can utilize its end-to-end encryption when making private phone calls or when having secret chats. In addition to encryption and privacy settings, Telegram offers a strict pledge to "disclose 0 bytes of user data to third parties, including governments." Furthermore, Telegram places their physical cloud servers around the world to prevent any particular government or authority from having sole jurisdiction.[1,2]

A study by the George Washington University Program on Extremism finds that the features offered by Telegram are often exploited by extremist groups, and the application is described as "the centerpiece of IS supporters' online communications strategy." Telegram is currently considered the preferred digital communication tool for IS sympathizers. Telegram is preferred because of its encryption capabilities as well as its public accessibility. Its features allow for a massive amount of content sharing and serves as a stable online platform for pro-IS content, an ecosystem for building extremist networks, an effective and secure internal communications tool, and a forum for recruiting new IS members. In recent years, IS has used Telegram to organize terrorism plots, disseminate propaganda, and claim responsibility for attacks. Telegram also hosts channels operating on behalf of other internationally recognized terrorist organizations to include al-Qaeda, the Nusra Front, Hamas, Hezbollah, and the Taliban.[1,2,6]

Neo-Nazis, white nationalists, and antigovernment extremists use Telegram to share propaganda advocating terrorism and mass shooting. The Southern Poverty Law Center examined publicly visible posts on the messaging app in which channel moderators urge their followers to "destabilize the US," "kill the cops," "shoot lawmakers" and attack synagogues, mosques and other houses of worship. People in these same Telegram channels frequently post memes glorifying terrorists such as Anders Breivik, the man who killed 77 people in a Norwegian terror attack in 2011, Dylann Roof, a South Carolina man who murdered nine black churchgoers in 2015, Robert Bowers, who has been charged with federal hate crimes after 11 people were killed in a Pittsburgh synagogue shooting in 2018, and the man who stands accused of killing 51 Muslims in Christchurch, New Zealand, in March 2019. Telegram users in channels that promote terror also discuss weaponry, including the subject of building guns with 3D printers and homemade methods.[3]

Signal

Signal is one of many encrypted messaging services, but it stands out for its commitment to security and ease of use. The chat service retains virtually no information from users, including messages and address books, on its servers. Messages also remain encrypted when passing through Signal's servers, meaning that the app's creators can't read them. Only the person who receives

the message holds the key to decrypt and read it. If a government agency had a wiretapping order for a Signal message, the key to decipher the messages would still not be accessible. [4]

WhatsApp, Facebook's Messenger and Google embedded Signal's encrypted messaging system into their own apps in 2016. However, the privacy policy of each of these platforms is generally less private than that of Signal. While there is limited information available on extremists' use of Signal, the application is committed to privacy and freely accessible via a phone app or on a computer. It is reasonable to assess this platform's security features may be exploited by extremist groups both now and in the future.

WhatsApp

In 2018 WhatsApp was the most-popular messaging app in the world with 1.5 billion users in 180 countries. However, when Facebook acquired WhatsApp in 2014, Telegram attracted millions of new users. This was due in part by concerns regarding changes in privacy policy and information tracking. While WhatsApp also uses Signal's encryption, WhatsApp may retain some data on conversations. This includes the phone numbers used and the times that the messages were sent. WhatsApp also regularly accesses personal contact lists.[4,5]

Case Studies

November 2015

A series of coordinated terrorist attacks took place across Paris, including 4 suicide bombings, mass shootings, and a hostage stand-off. IS claimed responsibility for the attacks that killed 130 people and wounded more than 350 others. French investigators reported that the assailants used chats on Telegram and WhatsApp to plan and coordinate the attacks.[10]

July 2016

Ten members of a pro-IS cell were arrested in Brazil after allegedly plotting terrorist attacks against gays, Shiite Muslims, Jews, and foreigners at the 2016 Olympics in Rio de Janeiro. According to prosecutors, members of the cell had communicated with each other over various platforms including Telegram, where they had discussed training, how to obtain weapons, and plans for carrying out attacks.[6]

June 2017

Inspired by IS, 3 occupants of a van drove through pedestrians on the London Bridge, before exiting and stabbing nearby pedestrians. Eight deaths and 48 injuries were reported. The ringleader of the "London Bridge" attack was a WhatsApp user, sending messages on the encrypted platform minutes before the attack. Authorities have been unable to access his account and messages due to the app's security policy. They have suggested that the attacker's use of WhatsApp enabled the plot to go undetected.[7]

May 2019

Private messages shared by the small far-right neo-fascist organization The Proud Boys on Telegram were recently leaked. In these messages, members discussed injuring and even killing their adversaries, plotting tactics and the optics of asserting a claim of self-defense if charged. A rally was planned in the chat that was later cancelled. While no attack has been carried out, this is an example of the far-right extremist rhetoric and tactic sharing encouraged and enabled by encrypted messaging platforms.[13]

Outlook

Social media companies are having to decide how to maintain an open speech platform when faced with posts by terrorist organizations or posts calling for violence. The massive amount of information and accounts prevents the companies from being able to consistently monitor the content posted. Extremist groups and individuals have used this to their advantage, tapping into global networks of support and spreading propaganda on an unprecedented scale. Additionally, the increase in use of encrypted messaging services has reignited the debate between tech companies and national intelligence as they seek to balance privacy and security. As these services increase in popularity, governments will continue to adapt their policies, in hopes of detecting future attacks. However, even as some accounts or sites shut down, communities of extremists will likely simply shift to other websites and platforms. Social media and encrypted messaging will continue to be exploited by international terrorist groups, small domestic extremist groups, and any extremist individual seeking a platform or community of support.

Source List

1. The George Washington University Program on Extremism. *Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram.*
2. Center for Homeland Defense and Security. *Islamic Extremism on Telegram.* https://www.hsdl.org/c/islamic-extremism-on-telegram/.
3. The Southern Poverty Law Center. *Far-Right Extremists Are Calling for Terrorism on the Messaging App Telegram.* https://www.splcenter.org/hatewatch/2019/06/27/far-right-extremists-are-calling-terrorism-messaging-app-telegram.
4. The New York Times. *Worried About the Privacy of Your Messages? Download Signal.* https://www.nytimes.com/2016/12/07/technology/personaltech/worried-about-the-privacy-of-your-messages-download-signal.html?module=inline.
5. Business of Apps. *WhatsApp Revenue and Usage Statistics*. 2019. https://www.businessofapps.com/data/whatsapp-statistics/.
6. Counter Extremism Project. *Terrorist on Telegram.* https://www.counterextremism.com/terrorists-on-telegram.
7. The Times. *London Bridge Attack.* https://www.thetimes.co.uk/article/london-bridge-terror-attack-planned-on-whatsapp-32r38jz8v.
8. Associated Press. *8chan Owner Heading to US as Lawmakers Seek Answers.* https://apnews.com/d1a1ba8d3cf24202b5c45815b05c441d.
9. The Washington Post. *Three Mass Shootings This Year Began with a Hateful Screed on 8chan. Its Founder Calls It a Terrorist Refuge in Plain Sight.* https://washingtonpost.com/technology/2019/08/04/three-mass-shootings-this-year-began-with-hateful-screed-chan-its-founder-calls-it-terrorist-refuge-plain-sight/.
10. The Hill. *Officials: Paris Attackers Used Encrypted Apps.* https://thehill.com/policy/cybersecurity/263640-report-paris-attackers-planned-strikes-on-encrypted-apps.
11. The New York Times. *The Week in Tech: Do You Prefer Free Speech, or a Perfectly Clean Internet?* https://www.nytimes.com/2019/04/19/technology/terrorist-groups-social-media.html.

12. Combatting Terrorism Center at West Point. *Tweeting for the Caliphate: Twitter as the New Frontier for Jihadist Propaganda.* https://ctc.usma.edu/app/uploads/2013/06/CTCSentinel-Vol6Iss62.pdf.
13. HuffPost. *Leaked Proud Boys Chats Show Members Plotting Violence at Rallies.* https://www.huffpost.com/entry/proud-boys-chat-logs-premeditate-rally-violence-in-leaked-chats_n_5ce1e231e4b00e035b928683